IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131143

A Wi-Fi Disruptor in the Modern Age

Dr. Kiran P[1], Ayush Shanmukha[2], DS Sai Suhas[3], Umesh Kumar A[4]

Guide and Head of Department, CSE-CY, RNSIT, Bengaluru, India[1]

Student, CSE-CY, RNSIT, Bengaluru, India[2]

Student, CSE-CY, RNSIT, Bengaluru, India [3]

Student, CSE-CY, RNSIT, Bengaluru, India[4]

Abstract: The rapid development of Wi-Fi enabled devices is important in wireless network security. This research focuses on the design and implementation of a Wi-Fi jammer using NodeMCU (ESP8266) microcontroller that disrupts local Wi-Fi communication by exploiting vulnerabilities in IEEE 802.11 protocol. Jammers work by disrupting devices in the access point area by sending authentication packets. This paper describes the hardware and software of the project, including the configuration of ESP8266, firmware development, and how packet injection works. This study demonstrates the simplicity of manufacturing jamming devices, while also revealing their misuse and the ethics of using these systems. Finally, this work contributes to the broader field of wireless network security by providing insight into potential defenses to mitigate the effects of Wi-Fi network vulnerabilities.

Keywords: Wi-Fi, ESP8266 NodeMCU, OLED 0.96

I. INTRODUCTION

A Wi-Fi Disruptor is a device designed to disrupt wireless communications by emitting signals that block Wi-Fi communications. This device uses unlicensed frequencies, such as the 2.4 GHz and 5 GHz ranges commonly used by Wi-Fi networks. Wi-Fi Disruptors can disrupt legitimate signals by emitting noise or irregular packets on these frequencies, causing network outages or denial of service (DoS) attacks. While Wi-Fi Disruptors are sometimes used for security or to test connections in controlled environments, their misuse can lead to risks such as business disruption, breach of confidentiality, and blocking access to emergency services. Understanding how they work is crucial to building effective defenses and securing wireless communications.

II. LITERATURE REVIEW

A. Denial of Service in 802.11 Wireless Networks: Attacks” by Bellardo, J., & Savage, S. USENIX Security Symposium, 2003

This early paper discusses various denial-of-service (DoS) attacks in Wi-Fi networks, focusing on deauthentication and disassociation attacks. Despite predating the ESP8266, it offers foundational insights into the protocol vulnerabilities that these attacks exploit.

B. A Survey on Security and Privacy Issues in Modern Wi-Fi-enabled IoT Devices” by Raza, S., Wallgren, L., & Voigt, T. EURASIP Journal,2018.

This survey examines security and privacy risks in IoT, particularly for Wi-Fi-enabled devices like the ESP8266. It highlights deauthentication and DoS attacks as significant threats and suggests potential mitigations for these vulnerabilities.

C. Security and Privacy Issues in IoT Device Interactions: Challenges and Solutions "by Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. IEEE Internet of Things Journal, 2015.

While not focusing specifically on deauthentication, this paper addresses security vulnerabilities in IoT devices, including the ESP8266. It offers insights into common attacks and the security challenges associated with low-cost microcontrollers.

DOI: 10.17148/IJARCCE.2024.131143

D. Ethical Hacking and Legal Aspects in IoT Security Testing” Kesan, J., & Zhang, C. Cybersecurity and Privacy, 2020.

This paper addresses the ethics and legalities of network testing and hacking tools, including Wi-Fi deauthing. It emphasizes the responsible use of tools like the ESP8266 deauther for educational and security research purposes.

E. Experimental IoT Penetration Testing Platform Using Low-cost Hardware”, Helder, F., & Vega, M. International Journal of Engineering and Technology, 2020.

This paper explores the use of ESP8266 microcontrollers for penetration testing on Wi-Fi networks, demonstrating deauthentication and other attacks. It offers a methodology for conducting ethical testing with the device.

III. Wi-Fi (Wireless Fidelity)

A. What is Wi-Fi

Wi-Fi is the backbone of connectivity for most gadgets as it enables them to communicate with each other and the Identify applicable funding agency here. If none, delete this. Internet. It is because of Wi-Fi that smartphones, laptops, tablets, and other portable devices are able to easily operate on the web, stream content, and communicate with others. Such smart home devices as Amazon Echo or Google Nest, Wi-Fi thermostats, and others rely on wireless networks for automation, security and control of the home. Even entertainment devices such as Smart TVs [2] and streaming classic devices like Roku and Fire Stick utilize Wi-Fi to provide users with sophisticated content. Similarly, we have watches and devices that are smart and help in keeping fitness data synchronized to enhance the usability and logistics as well as productive factors of the users. Passengers in a modern vehicle can Wi-Fi connect the vehicle to control functions of the car. There is also the monitoring and emergency medical equipment that can be considered remotely operated that uses Wi-Fi to convey sensitive health information. All this is indicative of the fact that there is a growing trend in the reliance on Wi-fi to help enhance communication. Another factor to consider is that Wi-Fi 6 and the yet to be released Wi-Fi 7 also assist in providing better connection with higher speeds and larger bandwidth.

B. Wi-Fi IEEE 802.11

The range of Wireless Local Area Networks, better known as Wi-Fi, is detailed in the IEEE802.11 standard. It was introduced in 1997 but has been reviewed and enhanced in subsequent iterations to include updates on speed, reliability, and performance. The encompass the frequency ranges of 2.4 GHz, 5 GHz, and most recently 6 GHz, there are multiple modes intended for the different operating applications. Widespread also the boundaries of the Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), and Wi-Fi 6 (802.11ax) improvement that allows operating efficiently in over-clouded areas. As for the current time, it is slated that Wi-Fi 7 (802.11be), which is expected to finish in 2024 is capable of supporting speeds of up to 30 Gbps believe this will improve the networks utility and capabilities. The transition from devices such as mobile phones and computers to the IoT and devices. It is possible to modify it even here and there to some extent without any strain on any features. A progression of the 802.11 standard has brought to the world of Wi-Fi also such remarkable technologies as MUMIMO, beamforming, and even greater spectral efficiency. Each new version aims to build on the previous one in order for it to be in tandem with the ever-changing world of wireless communication. I

IV. WI-FI DISRUPTION

A Wi-Fi outage is the term used to define loss or break in wireless connectivity in which a device becomes unable to connect itself or transfer any messages. This could be caused by such events as microwaves, Bluetooth or high traffic. Vandalism involves even such cybercrimes as DoS attack, or even authentication, which is flooding or taking over a device from the attacker’s domain. Such calamities can lower the quality of service, create a bad experience for the users, and even elements like healthcare service and emergency services. These problems can be dealt with by using modern communication methods including combating interference and protection strategies to realise effective communication.

A. Impact of Disruption

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁒ Peer-reviewed & Refereed journal ⁒ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131143

• Poor Network Performance: Outages will give a detrimental effect causing the network's speed to decrease, bandwidth to be restricted and connectivity lost which affects the user in regards to performing work, streaming or accessing the web.

• Decreased Productivity: Any business or individual that has a requirement for video conferencing, cloud computing or video transferring via wi-fi has experienced, which brings about a decrease in productivity • Effects on essential systems: Outages interfere with essential services such as that of health and security and even emergency communication systems.

• User Discontent and Connectivity Loss: Users encounter intermittent connectivity problems owing to Wi-Fi outages which leads to user frustration, and service cancellation or the operations being postponed until the time when connectivity is restored.

• Exposure to further attacks: Network Security breaches may make the systems even more vulnerable as the attackers may take advantage of the downtime and penetrate or destroy the systems.

• Disruption of smart appliances: On Static Wi-Fi interference will have an adverse effect on the performance of the smart appliances such as home appliance, smart devices and IoT which may cause the body to malfunction or fail altogether.

B. Uses of Disruption

• Security Testing: On occasion, controlled Wi-Fi interference is utilized when determining just how tough networks can be. During such events, some network managers may purposely interfere, for example, with a DoS attack to identify security weaknesses and strengthen the security stepped against any future cybersecurity attacks before they happen.

• Preventing Unauthorized Access: In some situations, it may be necessary to intentionally interfere with a Wi-Fi network to prevent unauthorized access, especially where the network is under internal or external cyber-attack. Interfering with the access of Wi-Fi can help create the window period whilst the IT teams enforce security protocols or disable malicious activities.

• Protection Security: In government institutions, corporate office settings, and other similar sensitive environments, Wi-Fi interference can be used as a countermeasure to prevent any unwanted surveillance and data collection especially potential hostile actor's interference communications.

• Controlling Network Usage: On instances of educational institutions, places of the public, and office settings, purposeful Wi-Fi disturbance can control the excessive use of a network during peak hours. This is helpful in controlling transmission.

C. Denial of Service Attack

A denial of service (DoS) attack [1] is an attempt to temporarily or permanently make a machine or network unavailable to intended users by a large number of site visitors. Therefore, it makes it unusable by flooding this server with too many requests. to use resources such as CPU bandwidth or memory It may cause more complex service crashes or slowdowns. A type called distributed denial of service (DDoS) employs multiple machines to carry out an attack. This often involves botnets, which are difficult to signal and mitigate attacks. This can cause significant damages, such as financial loss. reputational damage and discontinuation of service Mitigation measures include firewalls. Cost Limitation and a special DDoS protection service that filters malicious traffic before it reaches the system.

D. Rogue Access Points

A rogue access point (RAP) is an unauthorized Wi-Fi access point. This can pose a significant security threat. Attackers may intend to capture or control an organization’s activities. or strategically positioned by customers who have no internal knowledge of the organization These incendiary points can trap devices as interfaces for them. Instead of a real organization which pushes for a medium attack

E. Free Wi-Fi points

Using free, open Wi-Fi to draw attention to certain security threats to customers that were not exposed Man-in-the-Middle (MITM) attacks allow programmers to intercept communications between devices and systems. Get sensitive information like passwords or credit card information, free Wi-Fi, and rebels enter the spotlight. Where attackers connect customers to compromise their devices. . . They set up a fake system to trap them into doing just that. Another threat is data sniffing, where attackers monitor decryption activity to grab personal information. Open systems often require accurate encryption. and may not have authority for Malware spread This allows malicious programs to be sent to connected devices. Additionally, free Wi-Fi increases the chance of session hijacking. Where attackers can intercept dynamic sessions, using VPN can help filter out these threats by ensuring HTTPS encryption.

V. MAIN HARDWARE COMPONENTS

A. ESP8266 Wi-Fi module

The ESP8266 is one of the cheap Wi-Fi modules made by Espresso Systems, intended to add wireless connectivity to microcontroller-based projects. It supports the IEEE 802.11 b/g/n standards, which allow devices to connect to wireless networks for communication. It is also self-contained making external components unnecessary thanks to the incorporation of a microcontroller and a Wi-Fi chip in the module. It has different variants including the ESP-01 and ESP-12 giving it versatility for a range of IoT applications. The ESP8266 is known for its small size and low power consumption, as well as its ability to work with other platforms such as Arduino. It is suitable for monitoring, automation, and IoT systems. It also can easily be programmed with basic codes to interact with sensors and devices making it very easy to use for engineers and developers.

B. OLED 0.96in Display

The 0.96-inch OLED show: it is a little show screen with 128x64 pixels resolution that is typically used in embedded systems because it is a high-resolution display. It is based on OLED technology which has the benefit of using lesser power and produces brighter colors and black which make the screen more visually appealing. Such display modules are designed to utilize I2C or SPI communication protocols to easily interface with microcontrollers e.g. Arduino and Raspberry pi. Because of its size it can be employed in performing tasks such as displaying digital clocks or readings from sensors significantly saving space. Besides, its clear display and very low power consumption rates make it one of the most desired devices for multiple Do It Yourself (DIY) gadgets applications.

C. Arduino IDE

The Arduino based developments are very well supported through software in the form of Arduino Integrated Development Environment (IDE). A platform that allows users to easily write compile and upload code for their microcontroller-based projects. The IDE is C/C++ based and supports multiple libraries for various sensors, motors or shields easing the development process for everyone including beginners and experts. It has sequential debugging tools, code uploading facilities and simulation features before a code is actually uploaded onto the physical board.

DOI: 10.17148/IJARCCE.2024.131143

VI. METHODOLOGY

A. Module Design and Components

The ESP8266 module acts as the central controller of the system. This has been fixed to interfere with Wi-Fi by sending authentication revocation packets. These bundles target the enterprise and separate devices from the enterprise. 0.96-inch OLED display is used to highlight real-time information such as interrupter status and hot Wi-Fi access points by Communicates with ESP8266 via I2C, allowing integration It’s easy to use a static control source such as a lithium-ion battery or USB to control the ESP8266, which operates at 3.3V, which guarantees reliable performance...

B. Software Setup

The Arduino IDE is used to program the ESP8266 for Wi-Fi disabling. Libraries such as ESP8266 Wi-Fi, Wi-Fi UDP and Adafruit SSD1306 form the core of Wi-Fi communication, sending certification reduction packages. and OLED display control, fault code will send parcel disconnect authentication which causes the target system to fall out These combinations work until a connected device is forcibly disconnected. The OLEDs demonstrate the sophistication of attack status, Wi-Fi points of interest, and notifications.

C. Testing and Troubleshooting

After uploading the code to the ESP8266, use the serial screen to check for errors and ensure communications are working properly. The OLED display must modify in real time to show the status of the ESP8266. Blockers or network problems Test the interrupter in a controlled environment. and confirm that the device can be disconnected from the target organization There is no doubt that the framework behaves as expected without noise measurement on unsupervised systems. Fixed issues such as incorrect performance or network issues during testing.

D. Ethical Considerations

Using Wi-Fi Disruptors is illegal[4] in many countries. By including the states that form the group together. Regulated by the FCC, these rules are in place to avoid barriers to basic communications such as crisis management. Wi-Fi disruptors have recently been created and deployed. It is important to follow the rules regarding far-field impedance. Untrustworthy use of such frameworks can lead to legal consequences and harm others. It is guaranteed that moral duty and compliance with the law take precedence in the performance of such innovations.

VII. CONCLUSION

We’ve created a Wi-Fi disruptor that provides individuals with a level of total security against miscreants or to gain unfettered attention. This can be misused by attackers to gain unauthorized access to their framework. This personal blocker works by blocking unwanted signals from suspicious systems. Helping individuals protect their organizations. Using this tool, people can circumvent destructive systems and guarantee an interface to a reliable Wi-Fi source. In the end This deterrent provides a common-sense system to guarantee personal equipment against destructive attacks in open areas. The system’s simplicity and adequacy make it a useful tool for improving remote security in normal situations.

VIII. REFERENCES

1. “Denial of Service in 802.11 Wireless Networks: Attacks” by Bellardo, J., Savage, S. USENIX Security Symposium, 2003.
2. “A Survey on Security and Privacy Issues in Modern Wi-Fi-enabled IoT Devices” by Raza, S., Wallgren, L., Voigt, T. EURASIP Journal,2018.
3. “Security and Privacy Issues in IoT Device Interactions: Challenges and Solutions” by Mahmoud, R., Yousuf, T., Aloul , F., Zualkernan, I. IEEE Internet of Things Journal, 2015.
4. “Ethical Hacking and Legal Aspects in IoT Security Testing” Kesan, J., Zhang, C. Cybersecurity and Privacy, 2020.
5. “Experimental IoT Penetration Testing Platform Using Low-cost Hardware”, Helder, F., Vega, M. International Journal of Engineering and Technology, 2020